IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Jorge ABELLAN SEVILLA et al. Serial No.: 10/561,012 Filed: December 11, 2006 For: Databases Synchronization	Examiner: Mahmood, Rezwanul Group Art: 2164 Conf. No.: 6077

Mail Stop **Appeal Brief - Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

SIR:

This is an appeal, pursuant to 37 C.F.R. § 41.37, from the decision of the Examiner in the above-identified application, as set forth in the Final Office Action dated February 11, 2011 wherein the Examiner finally rejected Appellant's claims. The rejected claims are reproduced in the Appendix A attached hereto. A Notice of Appeal was filed on June 10, 2011

Please charge the amount of $620.00 in payment of the government fee for filing an Appeal Brief pursuant to 37 C.F.R. § 41.20 to our Patent and Trademark Office Deposit Account No. 503111.

Appellants hereby petition for a two-month extension of the original shortened statutory response period set in the Notice of Panel Decision from Pre-Appeal Brief Review of July 20, 2011. Please charge our Patent and Trademark Office Deposit Account No. 503111 in the amount of $560.00 in payment of the government fee for a two-month extension of time so that the

period for response is extended to October 20, 2011.

Any additional fees or charges required at this time in connection with the present application may be charged to our Patent and Trademark Office Deposit Account No. 503111.

REAL PARTY IN INTEREST

The assignee, Axalto S.A., of applicants, Jorge ABELLAN SEVILLA and Christophe DUBOIS, is the real party of interest in the above-identified U.S. Patent Application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals and/or interferences related to the above-identified application at the present time.

STATUS OF CLAIMS

Claims 2-4, 6, 7, 10 and 11 have been rejected. Claims 2-4, 6, 7, 10 and 11 are on appeal.

STATUS OF AMENDMENTS

A Pre-Appeal Brief Request for Review was filed on June 10, 2011 subsequent to the Final Office Action. The Pre-Appeal Brief Request for review was considered by the panel of Examiners as noted in the Notice of Panel Decision from Pre-Appeal Brief Review mailed July 20, 2011, which maintained the rejection of claims 2-4, 6, 7, 10 and 11.

SUMMARY OF THE CLAIMED SUBJECT MATTER

A. Independent claim 10

Appellant's independent claim 10 is directed to a computer-implemented method for synchronizing, through a network, a first database that is stored in a mobile first data processing system and a second database stored in a second data processing system, the method comprising:

loading an application into a security token coupled to the mobile first data processing system, the application configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy (Specification as filed at p. 4, ll. 17-19; and at APP, CAR, MOB, DB1, DB2 and MNO in Fig. 1);

executing the loaded application in the security token (Specification as filed at p. 3, ll. 5-7 and p. 4, ll. 17-19; and at APP and CAR in Fig. 1);

receiving, by the application, messages or events that occur in the mobile first data processing system or in the network (Specification as filed at p. 4, ll. 21-24; and at CAR, APP and MOB in Fig. 1);

in response to the messages or events received and in accordance with the synchronization policy, concluding by the application, whether a synchronization of the first and second databases is needed (Specification as filed at p. 4, ll. 26-29; and at CAR, APP, DB1 and DB2 in Fig. 1), and

if a synchronization is needed, transmitting, by the application, a remote command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested, said remote command providing the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases (Specification as filed in p. 4, l. 31

-3-

through p. 5, l. 30; and at APP and MOB in Fig. 1); and

initiating, by the mobile first data processing system, the synchronization process

of the first and second databases in response to receiving the remote command (Specification as

filed at p. 5, l. 32 through p. 6, l. 2; and at MOB, DB1, DB2 and MNO in Fig. 1).

GROUNDS OF REJECTION TO BE REVIEWED IN APPEAL

1.   Whether claims 2-4, 6, 7, 10 and 11 are patentable under 35 U.S.C.

§103(a) over U.S. Patent No. 6,505,215 ("*Kruglikov*") in view of U.S. Patent No. 6,813,498

("*Durga*"), U.S. Patent No. 6,824,064 ("*Guthery*") and U.S. Patent No. 6,779,002 ("*Mwaura*").

2.   Whether claim 8 is patentable under 35 U.S.C. §103(a) over *Kruglikov*,

Durga, *Guthery* and *Mwaura* in view of U.S. Patent No. 6,676,022 ("*Guthery '022*").

ARGUMENT

1.   **REJECTION OF INDEPENDENT CLAIM 10, AND OF DEPENDENT CLAIMS 2-4, 6-8
       AND 11**

INDEPENDENT CLAIM 10
Independent claim 1 recites, *inter alia*, "a first database that is stored in a mobile

first data processing system", "loading an application into a security token coupled to the mobile

first data processing system, the application configured to remotely request that the mobile first

data processing system start a synchronization process of the first database with the second

database according to a synchronization policy", and "if a synchronization is needed,

transmitting, by the application, a remote command to the mobile first data processing system

that informs the mobile first data processing system that a new synchronization is requested, said

<u>remote</u> command providing the mobile first data processing system with information about

-4-

synchronization parameters for use in synchronizing content of the first and second databases". The combination of the Examiner-cited art <u>fails</u> to teach or suggest these limitations.

Appellants' disclosed embodiments are directed to the synchronization of a database contained in a mobile first data processing system with another database contained in a network operator server (i.e. the "second data processing system"). In accordance with the invention, an operator or network-supplied application is loaded into a security token, such as a SIM card, that is coupled to the mobile first data processing system. The application is operable to request that the mobile first data processing system start a synchronization process between the database stored in the mobile first data processing system and the database stored in the network operator server in accordance with a specific operator/network synchronization policy. The security token does <u>not</u> contain the database, i.e., the application and the database are <u>separate</u> and <u>located in different devices</u>. In other words, the application loaded in the security token provides a <u>remote</u> command to the mobile first data processing system to start the synchronization process. The security token is thus a third party to the system of the mobile first data processing system <u>and</u> to the network operator server. A user of the mobile first data processing system <u>cannot</u> start or initiate synchronization for any database in the mobile first data processing system because such control is located <u>remotely</u>, in the application in the security token, from the mobile first data processing system (which contains the database). Synchronization is instead started automatically <u>by the security token</u>, which does <u>not</u> contain the database. However, it is <u>by operation of the application</u> that the messages or events that occur in the mobile first data processing system or in the network are received, and they are concluded <u>by the application</u>, in response to the messages or events received and in accordance with the synchronization policy, whether a synchronization of the first and second databases is needed.

Kruglikov discloses a system for synchronizing a portable system (110), e.g., a handheld device, with a personal computer (150). The Examiner concedes that *Kruglikov* does not disclose "the application configured to remotely request that a mobile data processing system start a process and receiving a remote command." (See the Final Office Action at page 3). The Examiner instead asserts that *Durga* discloses programming stored in a mobile unit configured to remotely start a process and receiving remote instructions.

Durga teaches that when a mobile unit has been reported to be missing, such as lost or stolen, an adjunct network entity, such as an intelligent network server, which has a detection and recovery application, determines or assigns a recovery identification and a recovery channel for the missing mobile unit. The mobile switching center then transmits a distinctive recovery page to the mobile unit via the base station, in which the recovery page includes information specifying the recovery identification and the recovery channel. The mobile unit, upon reception of the recovery page, enters a recovery mode and transmits a recovery signal on the recovery channel, with the recovery signal including the recovery identification. (See col. 1, line 63 through col. 2, line 11 of *Durga*).

But the programming stored in *Durga's* mobile unit is <u>not</u> configured to <u>remotely request</u> that the mobile unit start a synchronization process of the mobile unit with the mobile switching center. Indeed, the Examiner acknowledges that the programming is <u>stored in the mobile unit</u>. Moreover, the mobile unit enters the recovery mode and transmits the recovery signal on the recovery channel <u>upon reception of a recovery page</u>. Accordingly, the request to start the recovery process does not even come from the programming stored in the mobile unit in *Durga*; it comes instead from the completely separate and different detection and recovery application which is stored in the adjunct network entity via the mobile switching center. That

-6-

is, it comes from a completely separate data processing system, one <u>other</u> than the mobile unit, <u>that is not coupled to the mobile unit</u>. Nowhere does *Durga* identify or delineate an application configured to <u>remotely</u> <u>request</u> that the mobile unit start a synchronization process, wherein it is <u>by the application</u> that the messages or events that occur in the mobile unit or in the network are received, and wherein it is concluded <u>by the application,</u> in response to the messages or events received and in accordance with the synchronization policy, whether a synchronization of the first and second databases is needed.

Furthermore, the Examiner (at page 4 of the Final Office Action) acknowledges that *Kruglikov* and *Durga* do not explicitly disclose a security token coupled to the mobile first data processing device, and loading the application in the security token. The Examiner further cites *Guthery* as purportedly teaching "a security token coupled for communication with the mobile first data processing system and an application being loaded into the security token."

Guthery relates to a smart card capable of storing a number of applications and a memory that is logically partitioned into a number of memory blocks. *Guthery's* system seeks to allow simultaneous communication with more than one of the stored applications. To do so, it is necessary to dynamically allocate the scarce memory of the smartcard. This is done using a control program also stored on the smartcard. (See Abstract of *Guthery* and col. 2, lines 52-58).

Guthery does <u>not</u> address database synchronization and, therefore, does <u>not</u> teach or suggest "loading an application into a security token coupled to the mobile first data processing system, the application <u>configured</u> to <u>remotely</u> request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy" and "if a synchronization is needed, transmitting, by the application, a <u>remote</u> command to the mobile first data processing system that informs the

mobile first data processing system that a new synchronization is requested, said <u>remote</u> command providing the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases", as expressly recited in Appellants' independent claim 10. *Guthery*, therefore, does <u>not</u> in fact remedy the deficiencies of *Kruglikov* and *Durga*, discussed above, with respect to these claimed features.

Moreover, the Examiner contends that *Guthery* broadly teaches "loading the application in the security token." However, *Guthery* does not teach that <u>any</u> application can or should be loaded into the smartcard, as the Examiner suggests. Rather, *Guthery* simply teaches the use of multiple <u>conventional</u> security-related applications on a smart card, such as for use with credit card terminals, automated teller machines (ATMs), and mobile phones, with the additional inclusion on the smart card of a memory administration program that allows simultaneous communication with these various on-card applications while dynamically allocating the smartcard's <u>scarce</u> memory:

> The present invention provides tight linkage between the communication with smart card applications, allocation of scarce resources within the smart card, and the scheduling of execution of those applications. The system and method is constructed to embrace and be compatible with current modes of smart card usage. (Guthery at col. 7, lines 36-42).

Therefore, even assuming, *arguendo*, that *Kruglikov* and *Durga* disclose the claimed application "configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy," as the Examiner contends (which Appellants have fully refuted above), the combination of *Kruglikov*, *Durga* and *Guthery* would not teach or suggest a first database that is stored in a portable system <u>remote</u> from a <u>synchronization program loaded into the smartcard</u>, or

that a remote command is provided to the portable system from the smart card to start the synchronization process. Rather, this combination of references would, at most, teach the use of a smartcard as a security device, with the synchronization program being stored on the portable system, rather than in the smartcard, because that is where *Kruglikov* and *Durga* expressly teach that the synchronization program and recovery mode programming are stored, and *Guthery* fails to provide any teaching with respect to such a synchronization program.

Moreover, *Guthery* describes a plurality of applications that are run at the same time. In contrast, Appellants' claimed invention is directed to only a single application that transmits "a remote command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested". It is only after this synchronization that the mobile first data processing system, which stores the first database remotely from the application, initiates "the synchronization process of the first and second databases in response to receiving the remote command".

The third cited reference, *Mwaura*, discloses a computer software framework and method for synchronizing data across multiple databases involving the exchange of data synchronization messages. The Examiner cites *Mwaura* as purportedly teaching the receiving of a message by an application and determining if synchronization is needed by checking whether the message is relevant and, if so, taking a synchronization action. However, nothing has been found in *Mwaura* that would remedy the deficiencies of the combination of *Kruglikov* and *Guthery* with respect to the features of independent claim 10 discussed above.

Therefore, the Examiner's *prima facie* case in support of the rejection of independent claims 10 suffers from the additional deficiency that the cited references do not disclose the claimed features: "a first database that is stored in a mobile first data processing

system" and "loading an application into a security token coupled to the mobile first data processing system, the application configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy".

For the foregoing reasons, it is respectfully submitted that the combined teachings of *Kruglikov*, *Durga*, *Guthery* and *Mwaura* <u>fail</u> to establish a *prima facie* case of obviousness with regard to the subject matter recited in independent claim 10.

DEPENDENT CLAIMS 2-4, 6-8 AND 11

The fourth cited reference, *Guthery '022*, is cited by the Examiner as purportedly disclosing features of dependent claim 8. However, nothing has been found in *Guthery '022* that would remedy the deficiencies of the combination of *Kruglikov*, *Durga*, *Guthery* and *Mwaura* with respect to the features of independent claim 10 discussed above.

Dependent claims 2-4, 6-8 and 11 are thus deemed to be allowable for at least the same reasons as is independent claim 10.

For the foregoing reasons, it is submitted that the combined teachings of *Kruglikov*, *Durga*, *Guthery*, *Mwaura* and/or *Guthery '022* <u>fail</u> to establish a *prima facie* case of obviousness with regard to the subject matter recited in claims 2-4, 6-8, 10 and 11.

The Final Rejection of the claims in Group 1 should be reversed.

CONCLUSION

For the foregoing reasons, it is respectfully submitted that Appellant's claims are not anticipated or rendered obvious by the cited prior art and are therefore patentable over the art of record, and the Examiner's rejections should be reversed.

Respectfully submitted,
Cozen O'Connor

By   /Lance J. Lieberman/
          Lance J. Lieberman
          Reg. No. 28,437
          277 Park Avenue
          New York, New York 10172
          (212) 883-4900

Dated: October 20, 2011

CLAIMS APPENDIX

1.   (Canceled)

2.   (Previously Presented) The method according to claim 10, wherein the information includes an identifier of the second database to be synchronized.

3.   (Previously Presented) The method according to claim 10, wherein the information includes a synchronization protocol to be used between the first and second data processing systems.

4.   (Previously Presented) The method according to claim 10, wherein the information includes an identifier of the first database.

5.   (Canceled)

6.   (Previously Presented) The method according to claim 10, wherein the application is informed of a synchronization result between the first and second databases.

7.   (Previously Presented) The method according to claim 10, wherein the application is informed of a synchronization result if the synchronization result was requested in the command.

8.   (Previously Presented) The method according to claim 10, wherein the command is a card application toolkit command.

9.   (Canceled)

10.   (Previously Presented) A computer-implemented method for synchronizing, through a network, a first database that is stored in a mobile first data processing system and a second database stored in a second data processing system, the method comprising:

loading an application into a security token coupled to the mobile first data processing system, the application configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy;

executing the loaded application in the security token;

receiving, by the application, messages or events that occur in the mobile first data processing system or in the network;

in response to the messages or events received and in accordance with the synchronization policy, concluding by the application, whether a synchronization of the first and second databases is needed, and

if a synchronization is needed, transmitting, by the application, a remote command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested, said remote command providing the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases; and

initiating, by the mobile first data processing system, the synchronization process of the first and second databases in response to receiving the remote command.

11.   (Previously Presented) The method according to claim 10, wherein the mobile first

data processing equipment executes a program configured to receive all of the synchronization

parameters and to start the synchronization process.

12.   (Canceled)

NONE

RELATED PROCEEDINGS APPENDIX

NONE